

## UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of  
Information Associated with Apple ID  
"cefields2010@gmail.com" that is Stored at a Premises  
Controlled by Apple Inc.

Case No. 24-mj-579-PJC  
**FILED UNDER SEAL**

**FILED**  
SEP 10 2024  
Heidi D. Campbell, Clerk  
U.S. DISTRICT COURT

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).  
located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*

*Offense Description*

18 U.S.C. § 933(a)

- Firearms Trafficking

18 U.S.C. § 922(o)

- Illegal Possession of a Machine Gun

The application is based on these facts:

**See Affidavit of ATF SA Ben Nechiporenko, attached hereto.**

- ☒ Continued on the attached sheet.  
☒ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: 9/10/2025) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Ben Nechiporenko*

*Applicant's signature*

Ben Nechiporenko, ATF SA

*Printed name and title*

Subscribed and sworn to *in person* by *phone*:

Date: 9/10/24

*Judge's signature*

City and state: Tulsa, Oklahoma

Paul J. Cleary, U.S. Magistrate Judge

*Printed name and title*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of  
Information Associated with Apple ID  
“cefields2010@gmail.com” that is  
Stored at a Premises Controlled by  
Apple Inc.**

Case No. \_\_\_\_\_

**FILED UNDER SEAL**

**Affidavit in Support of an Application for a Search Warrant**

I, Ben Nechiporenko, being first duly sworn under oath, depose and state:

**Introduction and Agent Background**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at a premises owned, maintained, controlled, or operated by Apple Inc. (“Apple”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, in Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government information (including the content of communications) in its possession associated with the Apple ID “cefields2010@gmail.com” (Hereafter, “**TARGET ACCOUNT**”) as further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized

persons will review the information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent in Tulsa, Oklahoma since 2022. I am currently assigned to the Dallas Field Division, Tulsa Field Office with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). As a result of my employment with ATF, my duties include, but are not limited to, the investigation and enforcement of illegals use, possession, and trafficking of firearms, criminal organizations and gangs, arson, and illegal use and possession of explosives.

4. Prior to my tenure as an ATF Special Agent, I was a sworn law enforcement officer employed with the West Fargo Police Department in North Dakota from 2012 to 2022. During my employment with the West Fargo Police Department, my primary assignments included: Patrol Officer with the Patrol Division, Detective for the Metro Street Crimes Unit with the Special Investigations Division, Task Force Officer and Team Leader with U.S. Marshals Service High Plains Fugitive Task Force, and Patrol Sergeant with the Patrol Division. My training included over 1,250 hours of Police Officer Standards & Training (POST) approved training hours with an emphasis in gangs and narcotics enforcement. I served nine years with the

Army National Guard as a Combat Engineer and received an Honorable Discharge at the rank of Sergeant. I received a Bachelor of Science Degree in Criminal Justice from North Dakota State University in 2011.

5. As part of my duties as an ATF Special Agent, I investigate criminal violations in the Northern District of Oklahoma to include Title 18 U.S.C. §§ 933 – Firearms Trafficking and 18 U.S.C. §§ 922(o) – Possession of Machine Gun.

6. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

7. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 933 – Firearms Trafficking and 18 U.S.C. §§ 922(o) – Possession of Machine Gun, as described in Attachment B and is recorded on the device described in Attachment A.

### **Jurisdiction**

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

9. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Apple Inc. from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

### **Probable Cause**

10. On October 23, 2023, the Tulsa Police Department – Strategic Intervention Unit executed a state search warrant at Dai. L.’s apartment. TPD found Dai. L.’s cellphone, controlled substances and firearms, including multiple machine guns. One of the machine guns was reported stolen out of Washington County, Oklahoma on June 18, 2023. TPD arrested Dai. L. for multiple offenses including Possession of a Firearm by Adjudicated Delinquent, Trafficking in Illegal Drugs, Possession of a

Firearm while in the Commission of a Felony, and Possession of a Sawed-Off Rifle. A federal Grand Jury subsequently indicted Dai. L. in the Northern District of Oklahoma for Possession of Fentanyl with Intent to Distribute, Maintaining a Drug Involved Premises, Possession of Machine Gun (x2), Possession of Short-Barrel Rifle Not Registered in the NFRTR, and Possession of a Machine Gun in Furtherance of Drug Trafficking Crimes (x2). In December 2023, I obtained a search warrant (#23-MJ-639-JFJ) for Dai. L.'s cellphone. On April 5, 2024, Dai. L. pled guilty in federal court. Per Tulsa Police Department – Strategic Intervention Unit Investigator William Shanks, Dai. L. is a certified member of the criminal street gang, 52 Red Mob Gang Bloods.

11. On March 12, 2024, TPD-SIU arrested Don. L., a relative of Dai. L., for charges including Possession of a Firearm by an Adjudicated Delinquent, Obstruction, and an Application to Accelerate Warrant. A federal Grand Jury indicted Don. L. in the Northern District of Oklahoma for Possession of a Machine Gun, Firearms Trafficking, and Receiving a Firearm while Under Indictment. During the investigation, I obtained a federal search warrant (#24-MJ-290-MTS) for Don. L.'s Apple iCloud account. Per Tulsa Police Department – Strategic Intervention Unit Investigator William Shanks, Don. L. is a certified member of the criminal street gang, 52 Red Mob Gang Bloods. Since July 2023, Don. L. was under indictment in Muskogee County, Oklahoma for felony charges including Assault, Battery, or Assault & Battery with a Dangerous Weapon.

12. On July 23, 2024, I received information regarding Connor Evan FIELDS (DOB: XX/XX/2003; SSN: XXX-XX-3328) selling, and possibly manufacturing, machine gun conversion devices, machine guns, and firearms to individuals which included those federally prohibited from firearms possession and known criminal street gang members. Based on this information, I reviewed Don. L.'s and Dai. L.'s case files for any potential information related to FIELDS.

13. On July 24, 2024, Bureau of Alcohol, Tobacco, Firearms, & Explosives (ATF) Industry Operations Investigator (IOI) Todd Meztger searched the National Firearms Registration and Transfer Record; however, found no items registered to FIELDS nor his social security number.

14. On August 5, 2024, a federal Court Order (24-MJ-523-MTS) for Apple Inc. was issued in the Northern District of Oklahoma. On August 28, 2024, I received account information associated with (918) 859-1945 from Apple Inc. The data included the following account and subscriber information:

- Apple ID: cefields2010@gmail.com
- Directory Services Identifier (DSID): 18536311974
- Account Type: Full iCloud
- First Name: Connor
- Last Name: Fields
- Apple ID Creation Date: October 30, 2023
- Address: 21481 E 105<sup>th</sup> St S, Broken Arrow, Oklahoma 74014
- Phone: (918) 859-1945

15. On August 15, 2024, I reviewed phone extraction data from Dai. L.'s cell phone and the Apple iCloud data for Don. L.'s account. The data contained multiple

notable items related to Connor FIELDS including conversations and contact information across Instagram, iMessages, and Snapchat. I observed several conversations related to Connor FIELDS, including multiple firearm and machinegun conversion device transactions, in the data.

16. On September 10, 2023, text messages were exchanged between Dai. L. and Connor FIELDS' phone number, (918) 859-1945.

- Dai. L.
  - "Who this"
- (918) 859-1945:
  - "Connor"

17. On September 14, 2023, text messages are exchanged in a group chat which included Connor FIELDS, Dai. L., (918) 408-4896, and [keondrecreggett5@icloud.com](mailto:keondrecreggett5@icloud.com).

- Connor Fields:
  - "Twin what time u home"
- (918) 408-4896
  - "6"

- Connor Fields:
  - <https://m.made-in-china.com/product/Glock-17-18-19-G17-G18-G19-G26-G43-Sear-Tactical-Adjustment-CNC-Auto-Switch-1925834151.html>



•

*(Agent Note: Photograph of Machine Gun Conversion Devices commonly known as "Glock Switches")*

- "If y'all know anyone who wanna try an order"
- Keondrecreggett5@icloud.com
- "Ok"

18. The Machine Gun Conversion Device internet link FIELDS sends above directs to a website for Shenzhen Jiahao Xinda Technology Co., Ltd. On Shenzhen's corporate website<sup>1</sup> the corporation notes that all three of their manufacturing plants are in China, specifically Shenzhen, Jiangsu, and Dongguan. The Corporation also notes that it is an "export-oriented high-tech enterprise with products sold all over the world including America, Britain, Germany, Israel, Greece, Sweden, Malaysia, Australia, Russia, Japan Etc."

---

<sup>1</sup> <https://www.jiahaoxin.com/profile>

19. From October 4, 2023, to December 11, 2023, an Apple iOS iMessages conversation occurred between Don. L. and (918) 360-1433. I queried the phone number in TransUnion TLOxp and Accurant, and both showed the user as D.S. The conversations include D.S. arranging to purchase Machine Gun Conversion Devices from Don. L. Based on the dates, after the request from D.S., Don. L. contacted Connor FIELDS to acquire the Machine Gun Conversion Devices. Below are some of the notable statements made throughout the conversation.

*October 4, 2023 – 11:42am (UTC)*

- Don. L.:
  - “Send Addy”
- D.S.:
  - “2615 Oklahoma st”

*October 4, 2023 – 5:05pm (UTC)*

- D.S.:
  - “Ayy when u getting more”
- Don. L.:
  - “It’s gonna be a while until I get more”
- D.S.:
  - “Ight cause my button had broke” (*Agent Note: “Button” is a term used to describe a Machine Gun Conversion Device.*)
  - “The plastic mfka and I only got 200 so I was tap in when u got more”
- Don. L.:
  - “Yeah it’s not gonna break bro it’s metal”

- “It’s gonna be a while before I ever get more I’m just telling you know”
- “It’s what I got on my gun”
- D.S.:
  - “Bet ayy Ong hold that metal one till next Wednesday Ong”

October 22, 2023 – 1:19pm (UTC)

- D.S.:
  - “Tell dude that make em I need some flats too” (*Agent Note: “Flats” are likely a reference to Machine Gun Conversion Devices that do not protrude from the rear of the slide on Glock-style firearms.*)
- Don. L.:
  - “Bet”
- D.S.:
  - “How soon can he make ‘em”
- Don. L.:
  - “Now today”
- D.S.:
  - “Bet yk the deal hit me Wednesday wit prices:
  - “And I need another button for my 19” (*Agent Note: “19” is a model of Glock brand pistols.*)
- Don. L.:
  - “Bet”

October 25, 2023

- D.S.:
  - “You got them”

- Don. L.:
  - “Yuhh”
  - “His printer can’t make the flats tho I only got the fatback ones”  
*(Agent Note: “Flats” refers to an MCD which does not protrude from the rear of the Glock-style firearm. “Fatback” refers to a MCD which protrudes.)*
- D.S.:
  - “How much”

20. Beginning on October 24, 2023, at 4:14pm (Coordinated Universal Time), an Apple iOS iMessages conversation occurred between Don. L. and Connor FIELDS (918) 859-1945.

- Don. L.:
  - “Aye this Don call me back when you can”
- Connor Fields:
  - “Home in 15 where you wanna meet at”
- Don. L.:
  - “Bet”
  - “I’m not mobile til my girl get back but I’m north I’ll drop my pin bubba”
- Connor Fields:
  - “Bet”
- Don. L.:
  - “Bet”
  - “2207 N Rockford Ave Tulsa, OK 74106 United States”

- Connor Fields:
  - “Bet I’ll head that way here in few”
- Don. L.:
  - “Bet”
  - “How much you’ll charge me for 2-3??”
- Connor Fields:
  - “I’ll throw you 3 for a buck”
  - “W the stainless no sanding needed on them”
- Don. L.:
  - “Ion want the stainless”
  - “I want the other ones like the first metal one you gave me like 4-5 for like 50\$”
- Connor Fields:
  - “I don’t got aluminum ones no more but I’ll run you 3 stainless for 60 that’s as low as I can go on them ones I’ll send a pic on insta” (*Agent Note: “Insta” is a term used to describe the social media platform, Instagram.*)
- Don. L.:
  - “Ight bet can you bless me with 1 more bubba??”
- Connor Fields:
  - “Yeah that’s cool”
- Don. L.:
  - “Bet”
- Connor Fields:
  - “28 min out”

- Don. L.:
  - “Bet”
- Connor Fields:
  - “Here”
- Don. L.:
  - “Bet”
- Connor Fields:
  - “Done eating”
- Don. L.:
  - “Bet”

21. Beginning on November 8, 2023, at 11:33pm (UTC), an Apple iOS iMessages conversation occurred between Don. L. and Connor FIELDS (918) 859-1945.

- Don. L.:
  - *Photograph (Not Visible in Message Data)*
  - “ARP with 60 round” (*Agent Note: “ARP” is a term used to describe AR-style pistol firearms.*)
- Connor Fields:
  - “Hell yeah”
  - “I’ll have that deal ready I can meet you somewhere tomorrow”
- Don. L.:
  - “Bet”

22. Beginning on November 10, 2023, at 6:07pm (UTC), an Apple iOS iMessages conversation occurred between Don. L. and Connor FIELDS (918) 859-1945.

- Don. L.:
  - “You do it??”
- Connor Fields:
  - “Yeah it’s done”
- Don. L.:
  - “Lemme see”
- Connor Fields:
  - “Twin said you riding w us tomorrow so I was finna give it to you then”
- Don. L.:
  - “Bet”
- Connor Fields:
  - “Where you finna be in the Mornin so I can pick you up”
- Don. L.:
  - “North I’ll send addy”
- Connor Fields:
  - “Bet”
  - “Send addy I got couple stops to make so it’ll be a minute

23. Beginning on November 23, 2023, at 12:02am (UTC), a conversation occurred between Don. L. and Connor FIELDS (918) 859-1945.

- Don. L.:
  - “Let me know when you can get them in”
- Connor Fields:
  - “I’ll send you his info if shits legit”

24. Beginning on November 28, 2023, at 2:16pm (UTC), a conversation occurred between Don. L. and Connor FIELDS.

- Don. L.:
  - “What they on??”
- Connor Fields:
  - “I preordered they not shipped yet”
  - “I’m at work rn”
- Don. L.:
  - “Oh okay bet bet”
  - “Aye bro”
  - “You know someone that’ll trade my 5inch for 2gmans”  
*(Agent Note: “5inch” most likely refers to an AR-Style pistol with a 5-inch barrel and “gmans” refers to Glock brand pistols.)*
- Connor Fields:
  - “Not that I know of you might try the okc dudes”
- Don. L.:
  - “Okay bet”

25. Dai. L.’s Apple iOS Call/Facetime Logs included the following calls with Connor FIELDS’ phone number, (918) 859-1945:

- 09/10/2023: Incoming FaceTime Video

- 09/14/2023: Incoming FaceTime Video
- 09/18/2023: Outgoing FaceTime Video
- 09/18/2023: Incoming FaceTime Video
- 09/20/2023: Incoming FaceTime Video
- 09/23/2023: Incoming FaceTime Video
- 09/23/2023: Outgoing FaceTime Video
- 09/23/2023: Outgoing FaceTime Video
- 09/23/2023: Incoming FaceTime Video
- 09/23/2023: Incoming FaceTime Video
- 10/10/2023: Incoming FaceTime Video

26. On August 29, 2023, through September 6, 2023, Connor FIELDS' exchanged messages on Snapchat, with Dai. L.

- Connor Fields:
  - "1500\$ if you know anyone"



- 
- "Also got this for 800"

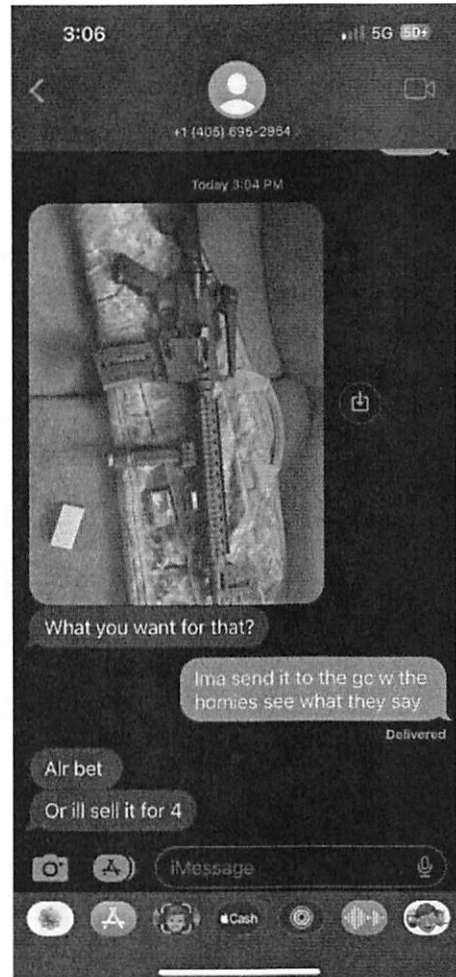
27. On October 17, 2023, Connor FIELDS' exchanged messages on Snapchat group chat which included Dai. L. (Benjuboydusse).

- Connor Fields:
  - "I got a g44 wa button for 400 if you know anyone got 2 mags with it 10 and 25 rd mags" (*Agent Note: Likely referring to a Glock Model 44, .22lr, with a Machine Gun Conversion Device. "Button" is a common term used to describe a Machine Gun Conversion Device.*)
- Benjuboydusse:
  - "Okay hold on"
- Connor Fields:
  - "Bet"

28. On October 17, 2023, Connor FIELDS' exchanged messages in a Snapchat group chat which included "benjuboydusse", "blockbender2300", "keepsteppnxx", and "luhtw1n".

- Connor Fields:
  - *No message content to display.*
  - *No message content to display.*
- Luhtw1n:
  - "Wats that"
- Connor Fields:
  - "26 w a 22 rd" (*Agent Note: Likely a reference to a Glock Model 26, .40S&W, with a twenty-two round capacity magazine*)
  - "Finna trade w Yatta tho"

- Luhtw1n:
  - “Aw then why you send it in here then”
- Connor Fields:
  - “He called me after I sent it”
  - *No message content to display*



- Luhtw1n:
  - “Who is that”
- Keepsteppnxx:
  - “What is it it loading”

- Luhtw1n:
  - “Ion even want that mf fr jus want tha 4grip”
  - “is that nay of tha oka Niggas we be fw?”
- Connor Fields:
  - “Yup”
  - “The skinny dude that told us to go get food while we wait on Z4”
  - “The gun a .22 not worth it imo”
- Blockbender2300:
  - “Yea that Mfa Trash To Me”
- Luhtw1n:
  - “Bro them niggas be havin some nasty shit”
  - “I won’t do nun for it either I’ll grab tho throw to one of tha brod”

29. Dai. L.’s phone extraction data included the following contacts related to Connor FIELDS:

- Snapchat: “Connor Fields”
  - User ID: fields.connor

30. Don. L.’s Apple iCloud data included the following contacts related to FIELDS.

- Instagram: fields\_\_connor “Connor Fields”
  - User ID: 36721356848

31. On August 5, 2024, a federal Court Order #24-MJ-522-MTS was issued for Instagram account "Fields\_\_Connor". I submitted the Court Order to Meta Platforms. On August 20, 2024, I received data from Meta regarding Instagram account "Fields\_\_Connor", and reviewed the data on August 21, 2024 which included the following information:

- Name: Connor Fields
- Vanity Name: fields\_\_connor
- Registered Email Address: cefields2010@gmail.com
- Registration Date: 05/27/2020
- Phone Number: (918) 859-1945

32. The data indicated Fields exchanged messages and calls with Instagram account "ffadon5ive\_two", a known account for Don. L., during the months September 2023, October 2023, January 2024, and February 2024.

33. On August 5, 2024, I served Meta Platforms, Inc. a federal Court Order ((#24-MJ-534-MTS) which had been issued in the Northern District of Oklahoma. On August 25, 2024, I received data from Meta Platforms, Inc. for Connor FIELDS Facebook account "100015225229195". The information included:

- Name: Connor Fields
- Phone Number: 19188591945
- Account Identifier: 100015225229195
- Email: cefields2010@gmail.com

34. I observed numerous internet protocol (IP) addresses with date/time stamps within the data. The IP addresses appeared to be primarily associated with Verizon Wireless, Cox Communications, and American Airlines. (*Agent Note: during my initial investigation into Connor FIELDS, I learned he is employed at Tulsa International Airport with American Airlines*). Many of the IP information sessions also included “Agent Strings” which indicated the device used to access Facebook was an Apple iPhone 14.

35. On August 23, 2024, I reviewed Tulsa Police Department Field Interview #2023-042581. The report indicated on August 31, 2023, officers were dispatched to 7022 South Mingo Road, Tulsa, Oklahoma regarding multiple males with an “RPG” and an “assault rifle”. Officers spoke with multiple males, including Connor FIELDS, who stated they were taking photographs in front of a business. FIELDS claimed the “RPG” [Rocket Propelled Grenade] was de-milled, and the Century Arms, model VSKA, serial #SV7133053, rifle was unloaded.

36. On August 26, 2024, I served Apple Inc. with a preservation request pursuant to 18 U.S.C. § 2703(f), requiring Apple Inc. to preserve all information associated with the account described in Attachment A.

37. I know “Glock Switch” style Machinegun Conversion Devices are classified as both Firearms and Machineguns as defined in 18 U.S.C. § 921(24) and 26 U.S.C. §§ 5845(a), (b). As they are “parts designed and intended solely and exclusively, or combination of parts designed and intended, for use in converting a weapon into a machine gun.”

### **Background Concerning Apple<sup>2</sup>**

38. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

39. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). The services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names including, but not limited to mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services

---

<sup>2</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

f. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

40. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

41. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

42. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

43. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

44. Apple provides users with approximately five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain

a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

45. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

46. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

47. Based on my training and experience, I know law enforcement can often retrieve messages and data deleted on Apple iPhones from iCloud back-ups. Further, stored communications and files connected to the targeted accounts may

provide direct evidence of the offenses under investigation. In addition to the actual content of said communications, the user's account activity, date-time logs, geo-location data, and other information retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is critical because it allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation, and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Alternatively, this same information may help to exclude the innocent from further suspicion.

48. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law

enforcement).

49. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

50. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **Information to be Searched and Things to be Seized**

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

52. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

53. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in

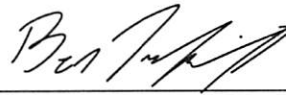
an account that are relevant to an investigation but do not contain any searched keywords.

### Conclusion

54. Based on the information above, I submit that there is probable cause to believe that there is evidence of violations of Title 18 U.S.C. §§ 933 – Firearms Trafficking and 18 U.S.C. §§ 922(o) – Possession of Machine Gun associated with the Apple “Target Account” described in Attachment A.

55. I request to be allowed to share this affidavit and the information obtained from this search (to include copies of digital media) with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,



---

Ben Nechiporenko  
Special Agent  
Bureau of Alcohol, Tobacco, Firearms,  
& Explosives

*in person*

Subscribed and sworn to ~~by phone~~ on September 10, 2024.



---

PAUL J. CLEARY  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to be Searched**

This warrant applies to information associated with the Apple ID  
“**cefields2010@gmail.com**”, that is stored at a premises owned, maintained,  
controlled, or operated by Apple Inc., a company headquartered at One Apple Park  
Way, Cupertino, California, 95014.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple Inc. (“Apple”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media

Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account May 1, 2023– Present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account May 1, 2023– Present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud account May 1, 2023– Present, including all iOS device backups, all Apple and third-party

app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers) account May 1, 2023– Present, including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations account from May 1, 2023, through present where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken between May 1, 2023– Present; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 18 U.S.C. §§ 933 – Firearms Trafficking and 18 U.S.C. §§ 922(o) – Possession of Machine Gun, including, for each account or identifier listed on Attachment A:

- a. Evidence indicating other accounts used by the owner of the Apple ID;
- b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and the account subscriber;
- d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- e. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple") and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. Such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature